A Privacy-Preserving Reliable Authentication Scheme for 6G-Enabled Internet of Vehicular Edge Computing Networks

Vijayalaxmi S. Sadlapur
REVA University, Bengaluru, Karnataka, India | Government Polytechnic, Zalaki, Vijayapura, Karnataka, India
vijayalaxmis_12@rediffmail.com (corresponding author)

Nayana Hegde
REVA University, Bangaluru, Karnataka, India
nayana.srikanth@gmail.com

Received: 16 April 2025 | Revised: 18 July 2025 and 4 September 2025 | Accepted: 6 September 2025

 DOI: https://doi.org/10.48084/etasr.11534

ABSTRACT

To meet the delay-awareness and compute-intensive requirements of the Internet of Vehicles (IoV) for providing smart driving assistance systems, the computational process is offloaded to different vehicles, Roadside Units (RSUs), or Vehicular Edge Computing (VEC) servers enabled by 6G networks. However, the untrustworthiness of node behavior makes meeting the security requirements and privacy constraints of vehicles a challenging task in 6G-enabled IoV edge networks. Recently, trust metrics have been designed to authenticate vehicles; however, the reliability of offloading aggregation has not been considered during the authentication process. This work introduces a novel edge-based aggregation model to improve fusion accuracy with higher noise levels to enhance vehicle privacy. A new approach, namely the Privacy-Preserving Reliable Authentication (PPRA) scheme, is proposed to support smart driving assistance systems. The PPRA scheme introduces an effective aggregation mechanism with higher noise levels and an incentive-based reputation model. Furthermore, a reliable authentication model is proposed to identify malicious and trusted vehicles. In addition, a Nash equilibrium game-based model is introduced to reduce communication failures in 6G-enabled Internet-of-VEC (IoVEC) networks. The PPRA scheme improves throughput and communication efficiency with minimal communication failures compared with the existing Enhanced Privacy-Preserving Security (EPPS) method.

Keywords-aggregation; delay; Internet of Vehicles (IoV); overhead; privacy; reputation metrics; Vehicle Ad Hoc Networks (VANETs); Vehicular Edge Computing (VEC)

I. INTRODUCTION

With the growth of wireless communication, information technology, artificial intelligence, and computationally delay-aware applications, the development of 6G-enabled Internet of Vehicles (IoV) networks has accelerated [1]. Similar to Vehicle Ad Hoc Networks (VANETs), the 6G-enabled IoV enables vehicles to connect with intermediate vehicles, infrastructure, and Roadside Units (RSUs); however, VANETs [2] do not support integration with cloud platforms. On the other side, the 6G-enabled IoV allows the integration of edge-servers and cloud platforms for collecting massive data and applying soft computing approaches [3] to support intelligent transport applications, such as route management, accident prevention, overtaking assistance, and traffic congestion management. The state-of-the-art architecture [4] requires data to be collected in a centralized server, leading to increased communication overhead and requiring larger computational resources. Thus, Vehicular Edge Computing (VEC), with a large number of edge devices in 6G-enabled IoV, is envisioned as a promising solution [5]. In IoV [6], different entities such as vehicles, pedestrians, smart sensors, communication modules, and computational platforms are involved, as these devices share information among themselves and the edge servers to enhance traffic efficiency and driving safety. However, centralized cloud-based systems may fail to meet the highly reliable and low-latency service requirements [7]. On the other hand, VEC enables the system to reduce communication costs and transmission delays and to enhance the Quality of Service (QoS) for vehicle users. The modern Smart Transport System (STS) involves different soft computing techniques to process compute-intensive data, such as image and video processing tasks either in VEC or cloud environments [8, 9].

The rapid evolution of 6G-enabled VEC networks has enabled efficient task offloading and real-time data processing,

significantly enhancing the capabilities of intelligent transportation systems. However, these advancements are hindered by critical security challenges arising from the inherent untrustworthiness of service devices [10]. VEC networks remain susceptible to various security threats, such as false-result attacks and collusion attacks [11]. As illustrated in Figure 1, malicious vehicles can engage in collusion to mislead task vehicles, causing them to rely on unreliable servers and thereby disrupting the vehicular system's functionality. Additionally, malicious service providers may deliberately return incorrect computational results, jeopardizing operational safety and potentially leading to severe traffic accidents with catastrophic consequences for drivers and passengers. Trust serves as the basis of network security [12], ensuring that applications operate within a secure and reliable environment. The trusted interaction problem in VEC networks has therefore become a pressing issue, attracting significant attention from both academia and industry [13].

Authors in [14] proposed a two-factor authentication mechanism to preserve vehicle privacy in IoV networks, combining a physical unclonable function-based authentication with an ideal session key exchange process. The model optimized authentication latency and communication overhead, ensuring high privacy and computational efficiency. However, it lacked scalability for large IoV deployments. Authors in [15] introduced a blockchain-based security mechanism with collaborative services for conditional privacy preservation. While enhancing transaction throughput and service latency, the reliance on blockchain imposed high computational costs, limiting real-time use. Authors in [16] developed a blockchain-enabled distributed authentication mechanism employing consensus and distributed ledgers to secure communication. It achieved high authentication success rates and low latency but consumed significant energy, restricting use in resource-constrained environments. Authors in [17] presented a task offloading strategy using digital twin-assisted intelligence with blockchain for secure task management [18, 19]. It improved task completion time and resource utilization but faced scalability issues due to computational complexity. Authors in [20] designed a secure offloading framework via Multi-Agent Reinforcement Learning (MARL) integrated with blockchain, improving offloading efficiency and data security. Yet, long training times limited real-time adaptability. Authors in [21] proposed Deep Reinforcement Learning (DRL)-based secure resource and task offloading with multi-slot optimization, enhancing task success and resource allocation. However, dependence on large training datasets reduced adaptability to unforeseen scenarios. Authors in [22] introduced a Multi-Stage Multi-Level Multi-Feature (MSMLMF) Stackelberg game for resource allocation and pricing in VEC, ensuring fairness and efficiency through contract incentives. Despite optimizing resource pricing fairness and budget utilization, the complex mathematical modeling incurred high computational overhead, limiting real-time application.

Existing trust mechanisms predominantly employ static identity authentication [14], blockchain [15, 16], and intrusion detection [17-19] technologies. However, these conventional methods exhibit inherent limitations when applied to the dynamic and complex aggregation task offloading scenarios in 6G-enabled VEC networks. Static identity authentication schemes provide trust validity only post-authentication, failing to adjust to the unpredictable and open nature of 6G-enabled VEC networks, which often involve selfish vehicles/servers [14, 16, 17]. Similarly, blockchain-based trust mechanisms, while benefiting from the immutability of blocks, face scalability issues as the transaction volume increases, consuming substantial storage and computational resources [20]. Intrusion detection-based trust strategies can identify explicit threats but struggle to predict possible security breach posed by untrusted vehicles [20, 21]. To enhance the security of offloading services, researchers have explored vehicle trust evaluation methods that provide more inclusive validation [21, 22].

Although these methods improve trustworthiness evaluations, they often overlook the efficiency of aggregation task offloading. This oversight can result in delayed service responses and significant communication overhead, undermining the performance and reliability of 6G-enabled VEC networks. Addressing these challenges necessitates a novel trust framework capable of balancing security with task offloading efficiency in the dynamic 6G-enabled VEC ecosystem. This study aims to develop innovative solutions that address the limitations of existing methods, ensuring robust, efficient, and scalable trust management for next-generation vehicular networks. The work introduces the Privacy-Preserving Reliable Authentication (PPRA) scheme for Internet-of-VEC (IoVEC) networks. The PPRA introduces an ideal aggregation mechanism to balance security and vehicle privacy constraints. The PPRA model ensures a reliable authentication scheme to identify malicious and non-malicious vehicles with minimal overhead while meeting security-privacy constraints. Finally, the PPRA introduces a Nash equilibrium game model to provide optimal security-privacy assurance. The significance of this research work is as follows:

- The PPRA ensures that vehicle privacy is maintained by resisting complex security attacks through the use of a higher-noise model in aggregation data.
- The PPRA ensures a reliable authentication mechanism using incentive-based reputation mechanisms that reduce overhead in IoVEC networks.
- The model assures optimal performance by employing a maximization function using a Nash equilibrium-based game model.
- The model is tested using realistic attack datasets, such as Denial of Service (DOS) and spoofing attacks.
- The results show that the PPRA improves overall throughput, enhances communication efficiency, and reduces communication failures compared with the existing Enhanced Privacy-Preserving Security (EPPS) method.

II. PROPOSED METHODOLOGY

This section introduces the proposed methodology of the PPRA model under the VEC framework, as shown in Figure 1. First, the system model describing the working process of the PPRA is presented. It then introduces a secure aggregation

model that ensures higher noise injection while satisfying vehicle security and privacy constraints, enabling VEC-based aggregation. The model incorporates a reliable authentication mechanism to distinguish between malicious and honest vehicles. Finally, a novel Nash equilibrium game model is introduced to achieve optimal performance, ensuring that both security and overhead constraints are satisfied and providing an efficient communication framework for IoVEC networks.

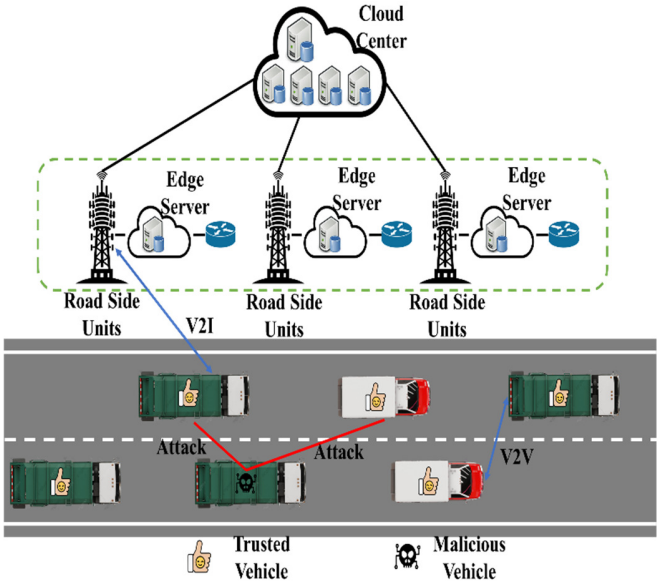

Fig. 1. Architecture of the VEC model for privacy-preserving authentication.

A. System Model

Let us consider an IoV network where vehicles are connected to RSUs or edge servers. The RSUs can perform simple data communication tasks; however, modern smart intelligence applications for IoV require integration with powerful servers by offloading computation to edge and cloud servers. As the connection between vehicles and edge servers is wireless in nature, they are prone to a wide-range of security attacks, such as DoS and spoofing attacks. Therefore, this work builds a secure aggregation model to authenticate vehicles and eliminate malicious vehicles from the IOV. A Nash equilibrium game-based security design is modeled to preserve vehicle privacy constraints.

The work considers a VEC server and a set of vehicles $X = \{x_1, x_2, x_3, \dots, x_P\}$, where all vehicles P generate a large amount of data, $Z = \{z_1, z_2, z_3, \dots, z_P\}$, and communicate them to the VEC server. This work uses normalized security reputation outcomes $t_k \in [0,1]$ to predict whether x_k is malicious or not. Thus, the VEC aggregates the information using following equation:

$$a = \frac{1}{P}\sum_{k=1}^{P} z_k \quad (1)$$

The information communicated by the vehicles is used to support both safety-critical and non-safety applications. The VEC performs average aggregation of sensitive vehicle information; thus, vehicle privacy constraints must be considered. The VEC can be compromised because the network contains both normal and malicious vehicles. As a result, malicious vehicles might communicate tampered information, and the VEC might leak sensitive data, potentially enabling spoofing attacks.

B. Secure Aggregation Model

This work introduces a secure aggregation model aimed at preserving vehicle privacy during communication in an IoV-VEC environment. The original sensor data collected from each vehicle at time step k are denoted by z_k. To ensure privacy, each data point is perturbed using additive Gaussian noise $\delta_k \sim N(0, \sigma^2)$, resulting in the noise-perturbed aggregated data $\tilde{z}_k$, expressed as:

$$\tilde{z}_k = z_k + \delta_k \quad (2)$$

where $\tilde{z}_k$ denotes the privacy-preserved version of the data communicated to the edge server. To aggregate data across P' vehicles while preserving privacy, the edge server uses an approximate aggregation function that operates over the noise-perturbed data. The aggregated result $\hat{a}^m$ at time step m is computed as:

$$\hat{a}^m = \sum_{k=1}^{P'} \tilde{y}_k^m \tilde{z}_k^m \quad (3)$$

where $\tilde{y}_k^m$ is a modified weight associated with vehicle k at time m, $\tilde{z}_k^m$ are the noise-perturbed data from vehicle k, and P' denotes the subset of valid vehicle data at that time. To further clarify the noisy input, (4) defines the perturbed data as a function:

$$\tilde{y}_k = O(z_k) = z_k + \delta_k \quad (4)$$

In (4), the random-noise generation is governed by the Gaussian distribution $O(.)$. However, the presence of noise complicates accurate aggregation and may affect privacy guarantees if improperly handled. To compensate for this, an incentive-based adjustment parameter ζ is introduced to refine the aggregated result and reduce the effect of noise:

$$\zeta = \left[\underline{a} - \hat{a}\right] \quad (5)$$

In (5), $\underline{a}$ represents the averaged aggregation of denoised estimates $\hat{z}_k$, and $\hat{a}$ is the approximation from (3). By using the adjustment parameter ζ, a corrected aggregation is computed as:

$$a^m = \sum_{k=1}^{P} y_k^m z_k^m \quad (6)$$

where y_k^m is the actual data weight or coefficient for vehicle k, and z_k^m are the original (non-noisy) vehicle data. This approach ensures enhanced privacy preservation while maintaining aggregation accuracy and system integrity.

C. Reliable Authentication Model

The aggregation outcome of the PPRA model using (6) ensures enhanced privacy preservation. Through position evaluation, if any attack occurs during transmission, the vehicle location where the attack has occurred can be identified. If an attack targets the transmitted information, the PPRA handles it using a state-change approach.

Consider two states of the transmitted information: J_0 representing the normal state and J_1 representing the attack state. The transition between these states is represented using conditional reputation probabilities:

$$R_h = R(J_1|J_0) \quad (7)$$

$$R_o = R(J_0|J_1) \quad (8)$$

Here, R_h denotes the probability that information transitions from the normal state J_0 to the attack state J_1, while R_o denotes the probability that information transitions from the attack state J_1 back to the normal state J_0.

From these state transitions, a variance N is computed to determine whether the information is in the normal state or attack state:

$$N = \| z_k^m - \hat{z}_k^m \|^2 \quad (9)$$

In (9), the variance N is evaluated by comparing the original transmitted data and the corresponding noisy transmission. Consider the data vector z_k as defined in (10):

$$z_k = (z_k^1, z_k^2, \ldots\ldots, z_k^p) \quad (10)$$

To identify attacks within the transmitted information, the threshold comparison $N \lessgtr_{J_1}^{J_0} (\vartheta)$ is used. If a significant change in the transmitted information is detected, the corresponding node (vehicle) is marked as malicious; otherwise, it is classified as a normal node. Mathematically, this is expressed as:

$$\hat{z}_k^m \leftarrow z_k^{m-1}, \text{ Else } \hat{z}_k^m \leftarrow z_k^m \quad (11)$$

Malicious packets induce additional computational overhead, leading to increased delay and potential data loss. Let I_0 denote the overhead of malicious packets and I_1 the overhead of non-malicious packets, where $I_0 > I_1 > 0$. The attack probability is denoted as R, which identifies attacks represented as $T(\vartheta, R)$. This is evaluated as:

$$T(\vartheta, R) = \left(I_1\left(1 - R_h(\vartheta)\right) - ER_h(\vartheta)\right)\left(1 - \sum_{k=1}^{P_o} r_k\right)T(\vartheta, R)$$

$$= \left(I_1\left(1 - R_h(\vartheta)\right) - ER_h(\vartheta)\right)\left(1 - \sum_{k=1}^{P_o} r_k\right) \quad (12)$$

In (12), the fusion (aggregation) is denoted as $U_{VEC}(\vartheta, R)$, where: $U_{VEC}(\vartheta, R) = T(\vartheta, R)$.

D. Nash Equilibrium Game-Based Security Design for Vehicular Edge Computing

To ensure a highly reliable model, the work introduces a game-theoretic framework based on Nash equilibrium. The Nash equilibrium is formulated to achieve optimal security, balancing vehicle privacy and overall security constraints. The model also ensures that each vehicle experiences a similar level of privacy-security assurance during the aggregation and authentication process.

The privacy-security game is modeled using parameters (ϑ^*, R^*), which guarantee the Nash equilibrium. The security upper limit ϑ^* is selected by the corresponding VEC to maximize $U_{VEC}(\vartheta, R^*)$ during the privacy-security assurance process. Simultaneously, attacker vehicles attempt to maximize their utility $U_{mr}(\vartheta^*, R)$. The privacy-security utility functions are defined as:

$$\vartheta^* = U_{VEC}(\vartheta, R^*) \quad (13)$$

$$R^* = U_{mr}(\vartheta^*, R) \quad (14)$$

The exclusive Nash equilibrium of the reliable authentication process in the aggregated data validation game is computed as:

$$\vartheta^* = G\big(I_1 - I_0 - R_h(\vartheta)(I_1 + I_0) + R_o(\vartheta)(I_0 + E)\big) \quad (15)$$

where E defines the overhead factor, I_1 represents reliable vehicles, and I_0 represents non-reliable vehicles. Algorithm 1 provides the complete set of steps involved in the proposed PPRA scheme.

Algorithm 1. PPRA
Input: Number of vehicles X, number of VEC servers A, variance of Gaussian noise σ^2, authentication threshold τ, and maximum game iterations T
Output: Authenticated vehicle set V_{auth} and malicious vehicle set V_{mal}
1. Initialize 6G-enabled IoV-VEC environment with X vehicles and A RSUs
2. For each vehicle $v_m \in X$:
3. Generate unique identifier $UID_m \leftarrow \text{Hash}(v_m||\text{timestamp})$
4: Send UID_m to nearest VEC for registration
5. VEC verifies UID_m and stores it in registration database R_{DB}
6. End for
7. For each vehicle $v_m \in X$:
8. Collect sensed data z_k^m from local sensors
9. Generate random Gaussian noise $\delta_k^m \sim N(0, \sigma^2)$
10. Compute noise-perturbed data: $\hat{z}_k^m = z_k^m + \delta_k^m$ using (2)
11. Send $(\hat{z}_k^m, UID_m)$ to the corresponding VEC
12. End for
13. VEC performs secure aggregation:
14. Compute incentive parameter: $\zeta = \left[\underline{a} - \hat{a}\right]$ using (5)
15. Apply privacy-aware fusion using ζ to update aggregated results
16. Perform reliable authentication:
17. For each received $\hat{z}_k^m$, verify trust score using (12)
18. If score $\geq \tau$ then
19. Add v_m to V_{auth}
20. Else
21. Add v_m to V_{mal}
22. End if

23. Execute game-theoretic optimization:
24. Initialize utility function $U_{privacy}$ and $U_{security}$
25. For $t = 1$ to T:
26. Vehicles select strategies to maximize $U_{privacy}$
27. VEC adjusts noise level/incentive to maximize $U_{security}$
28. Check convergence to Nash Equilibrium using (15)
29. End for
30. Output authenticated vehicle set V_{auth} and flagged malicious set V_{mal}

The proposed PPRA scheme operates in several key stages. In Steps 3 to 5, vehicle registration is performed via a secure UID hash sent to VEC. In Steps 8 to 10, Gaussian noise $\delta_k^m \sim N(0, \sigma^2)$ is generated for each vehicle. Steps 13 to 15, involve incentive-aware aggregation, which utilizes the feedback parameter $\zeta = \left[\underline{a} - \hat{a}\right]$ to update the aggregated results. In Steps 16 to 22, authentication decisions are made using trust scores calculated through (12). Finally, in Steps 23 to 29, the game-theoretic model ensures an optimal privacy-security trade-off through convergence to the Nash equilibrium. This security design provides a robust balance between high security and privacy while maintaining minimal computational overhead, increased throughput, improved communication efficiency, and reduced communication failures.

III. RESULTS AND DISCUSSION

This section evaluates the performance of the proposed PPRA scheme and compares it with the existing EPPS method [14], using a vehicular environment model based on the IoV-VEC framework described in [16, 17]. To ensure robustness and statistical reliability, a Monte Carlo simulation approach was employed. Each experiment was conducted over 10,000 independent iterations, accounting for stochastic variations in vehicle mobility, noise generation, and attack injection. The results are presented as mean $\pm$ standard deviation, and 95% confidence intervals were calculated using the student's t-distribution.

The performance of the proposed PPRA scheme and the baseline EPPS method was evaluated using three key metrics: overall throughput, communication efficiency, and communication failure rate. The simulation environment was constructed using the SIMITS simulator, which is an extended vehicular network simulation platform designed to model secure and high-throughput vehicular ad hoc communications with integrated 6G protocol features [23, 24]. SIMITS is built on top of the NS-3 simulation library, and it incorporates realistic urban and highway propagation models, supporting IEEE 802.11ad/ay and 6G gateway-level communication standards. For our simulation, the 6G communication characteristics such as mmWave channel modeling, high-capacity edge gateways, and Ultra-Reliable Low-Latency Communication (URLLC) were manually integrated into the NS-3 stack using modified PHY/MAC layer modules. This allows for emulation of 6G-compatible IoV-VEC network behavior. To support vehicle-edge interaction and privacy-preserved aggregation, custom modules were implemented for: simulating vehicle mobility patterns via SUMO, enabling data exchange with 6G gateway nodes using modified WaveNetDevice in NS-3, and handling privacy-aware data aggregation and encoding routines at the application layer. The communication visualization was provided through a custom-built C# dashboard, interfacing with NS-3 trace outputs to demonstrate vehicle-to-edge message flow, authentication status, and failure logs in real time. The SIMITS framework ensures that both physical-layer and application-layer parameters are realistically modeled in the context of IoV-VEC systems under 6G standards.

To evaluate the robustness of the proposed PPRA scheme under adversarial conditions, the work used the Canadian Institute of Cybersecurity (CIC) dataset [25], which includes labeled network traffic associated with realistic vehicular cyber-attacks. Specifically, we extracted and simulated the following IoV-relevant attack scenarios:

- DoS: Flooding packets to overload the edge server or network gateway, simulating adversaries disrupting Vehicle-to-Infrastructure (V2I) communication.
- Man-in-the-Middle (MITM): Injected spoofed data during vehicle-edge communication to test the authentication integrity of PPRA.
- Spoofing/impersonation attacks: Faked vehicle identities attempting to bypass privacy-preserving access control.

To simulate these attacks in the SIMITS/NS-3 environment, we extracted flow-level features (e.g., packet size, inter-arrival time, protocol, destination port) from the CIC dataset and mapped them to packet-level behaviors in our vehicular communication model. The DoS packets were recreated by introducing bursts of UDP traffic from compromised vehicle nodes to overload edge gateway queues. MITM and spoofing attacks were implemented via modified MAC and application layer scripts in NS-3 to inject fake authentication headers or malicious r_k values during aggregation. These attack models were then integrated into our simulation runs to compare how PPRA and EPPS handle intrusion attempts, in terms of throughput degradation, communication failure rate, and communication efficiency.

A. Throughput

This section evaluates the throughput achieved using the proposed PPRA scheme compared with the existing EPPS method. A higher throughput value indicates better performance. The throughput was measured by considering 50 vehicles moving at 50 m/s in a highway radio propagation environment. The results show that the proposed PPRA scheme achieved a higher throughput than the EPPS method across different Monte Carlo simulated sessions, as shown in Figure 2. The PPRA scheme improved throughput performance by 14.95% in comparison with the EPPS method. The enhanced throughput performance is attributed to the incentive-based aggregation model described in (5), which is applied during the authentication process to identify malicious and normal vehicles.

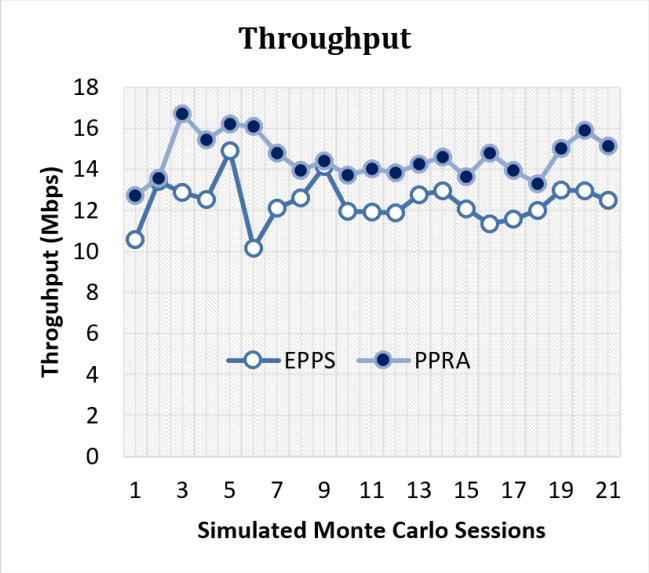

Fig. 2. Comparison of throughput between PPRA and EPPS.

B. *Communication Efficiency*

This section evaluates the communication efficiency achieved using proposed PPRA scheme compared with the existing EPPS method. The communication efficiency indicates how reliably packets are received by the RSU or the edge servers, where a higher value indicates enhanced performance. The communication efficiency was measured by considering 50 vehicles moving at 50 m/s in a highway radio propagation environment. The results show that the proposed PPRA scheme achieved a higher communication efficiency than the EPPS method across different Monte Carlo simulated sessions, as shown in Figure 3. The PPRA scheme improved communication efficiency by 25.4% in comparison with the EPPS method. This enhancement is attributed to the security model in (15), which uses the Nash equilibrium game framework.

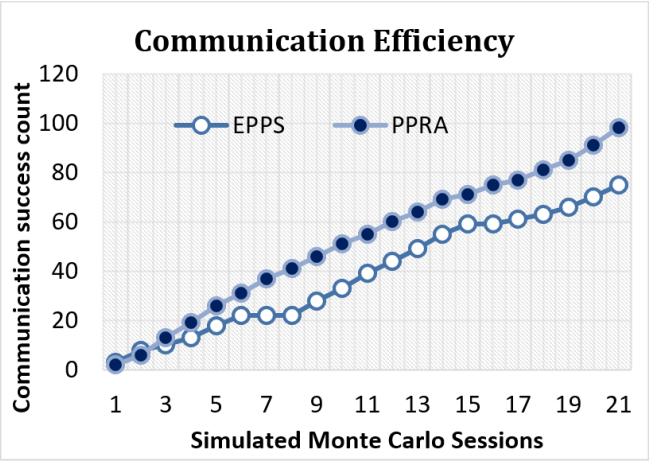

Fig. 3. Comparison of communication efficiency between PPRA and EPPS.

C. *Communication Failure*

This section evaluates the communication failure observed using the proposed PPRA scheme compared with the existing EPPS method. The communication failure indicates how often packet transmissions to the RSU or the edge servers fail, where a lower value represents better performance. The communication failure is measured by considering 50 vehicles moving at 50 m/s in a highway radio propagation environment. The results show that the proposed PPRA model achieved a lower communication failure count than the EPPS method across different Monte Carlo simulated sessions, as shown in Figure 4. The PPRA scheme reduced communication failure count by 31.37% in comparison with the EPPS method. This reduction is attributed to the reliable authentication model described in (12), which balances vehicle privacy preservation with overhead reduction.

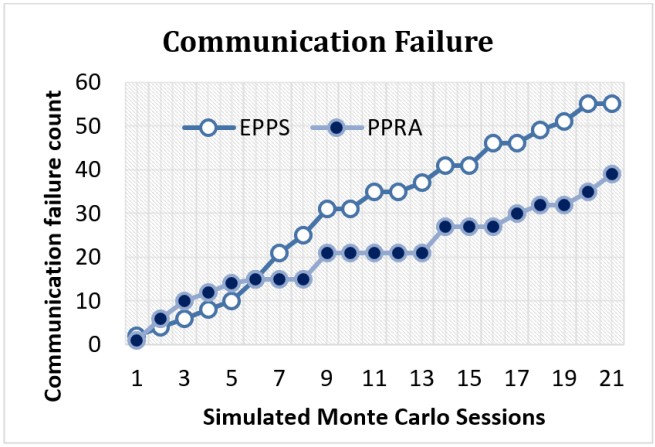

Fig. 4. Comparison of communication failure between PPRA and EPPS.

D. *Comparative Study*

The comparative study of PPRA and EPPS is presented in Table I. The PPRA model introduces a novel incentive mechanism, where a feedback-driven noise control parameter $\zeta = [\underline{a} - \hat{a}]$ dynamically adjusts the privacy-utility trade-off during aggregation. This ensures minimal loss of data quality while preserving vehicle privacy. PPRA incorporates a non-cooperative game-theoretic model between vehicles and edge servers, where vehicles aim to maximize privacy and reward, and the server aims to maximize data integrity and throughput. The system converges when vehicles settle on strategies that balance these trade-offs. The average number of iterations required to reach Nash equilibrium was ≤ 10, even with 50 vehicles and 5 edge nodes, thereby ensuring convergence behavior. Computational complexity grows linearly with node count, as the incentive utility function is localized, making the model suitable for large-scale, real-time deployment and ensuring better scalability compared with baseline models such as EPPS [14], Diffused Delegated Byzantine Fault Tolerance (d2BFT) [17], Multi-Agent DRL Secure Offloading (MADRL-SO) [20], and Filtered DRL Secure Offloading and Allocation (FDRL-SOA) [21].

TABLE I. COMPARATIVE STUDY OF PPRA WITH EXISTING VEC SECURITY AND AUTHENTICATION MODELS

Features	EPPS [14]	d2BFT [17]	MADRL-SO [20]	FDRL-SOA [21]	PPRA [proposed]
Noise type	Gaussian noise	Gaussian noise	No	Gaussian noise	Adaptive Gaussian noise
Authentication	Two-factor static model	DRL-based game theoretic model	Reputation contract using agent-based DRL	DRL-based behavior	Incentive-driven dynamic trust-aware game
Aggregation	Linear without noise control	No	No	No	Incentive-adjusted secure aggregation
Attack type	Limited to predefined signatures	No	Eavesdropping and selfish attacks	Eavesdropping	Spoofing, MITM, DoS
Computational complexity with limitations	Lowest complexity but weak adaptiveness	Polynomial, critic redundancy inflates cost	Heavy due to multi-agent RL training	Extremely high (deep RL with multi-slot optimization)	Moderate cost but reduces redundancy, improving scalability

IV. CONCLUSION

This study proposes an innovative edge-based aggregation framework designed to enhance fusion accuracy under high-noise conditions, thereby strengthening vehicular privacy. The Privacy-Preserving Reliable Authentication (PPRA) scheme introduced in this work establishes a robust foundation for smart driving assistance systems. By integrating an advanced aggregation mechanism with amplified noise levels and an incentive-driven reputation model, PPRA effectively ensures secure and efficient communication. Furthermore, the scheme incorporates a reliable authentication process capable of distinguishing between malicious and trustworthy vehicles, enhancing overall network integrity. To mitigate communication failures within the Internet-of-Vehicle Edge Computing (IoVEC) networks, a Nash equilibrium-based game model is employed, optimizing resource allocation and system stability. Comparative analysis demonstrates that PPRA significantly outperforms the existing Enhanced Privacy-Preserving Security (EPPS) approach, achieving improved throughput and communication efficiency while minimizing failure rates. This comprehensive approach underscores its potential to advance the development of privacy-preserving and resilient vehicular networks. The PPRA improved throughput performance by 14.95%, enhanced communication efficiency by 25.4%, and reduced communication failure by 31.37% compared with the EPPS method. Future work would consider enabling simultaneous assurance of both privacy and integrity constraints by employing more optimized iterative dynamic learning mechanisms to support complex, realistic workflow applications in IoVEC networks.

ACKNOWLEDGMENT

The authors sincerely thank REVA University for granting us the opportunity to carry out this research. The encouragement and support provided by the University greatly contributed to this work.

REFERENCES

[1] Y. Yigit, L. A. Maglaras, W. J. Buchanan, B. Canberk, H. Shin, and T. Q. Duong, "AI-Enhanced Digital Twin Framework for Cyber-Resilient 6G Internet of Vehicles Networks," *IEEE Internet of Things Journal*, vol. 11, no. 22, pp. 36168–36181, Nov. 2024, https://doi.org/10.1109/JIOT.2024.3455089.

[2] Y. Yigit, I. Panitsas, L. Maglaras, L. Tassiulas, and B. Canberk, "Cyber-Twin: Digital Twin-Boosted Autonomous Attack Detection for Vehicular Ad-Hoc Networks," in *ICC 2024 - IEEE International Conference on Communications*, Denver, CO, USA, 2024, pp. 2167–2172, https://doi.org/10.1109/ICC51166.2024.10622784.

[3] L. U. Khan *et al.*, "Federated Learning for Digital Twin-Based Vehicular Networks: Architecture and Challenges," *IEEE Wireless Communications*, vol. 31, no. 2, pp. 156–162, Apr. 2024, https://doi.org/10.1109/MWC.012.2200373.

[4] H. Guo, Y. Wang, J. Liu, and C. Liu, "Multi-UAV Cooperative Task Offloading and Resource Allocation in 5G Advanced and Beyond," *IEEE Transactions on Wireless Communications*, vol. 23, no. 1, pp. 347–359, Jan. 2024, https://doi.org/10.1109/TWC.2023.3277801.

[5] M. Deng *et al.*, "Reconfigurable Intelligent Surfaces Enabled Vehicular Communications: A Comprehensive Survey of Recent Advances and Future Challenges," *IEEE Transactions on Intelligent Vehicles*, 2024, https://doi.org/10.1109/TIV.2024.3476934.

[6] H. N. Abishu, A. M. Seid, R. H. Jhaveri, T. R. Gadekallu, A. Erbad, and M. Guizani, "Blockchain-Empowered Resource Allocation in HAPS-assisted IoV Digital Twin Networks: A Federated DRL Approach," *IEEE Transactions on Intelligent Vehicles*, 2024, https://doi.org/10.1109/TIV.2024.3492015.

[7] Q. Xie, Z. Sun, Q. Xie, and Z. Ding, "A Cross-Trusted Authority Authentication Protocol for Internet of Vehicles Based on Blockchain," *IEEE Access*, vol. 11, pp. 97840–97851, 2023, https://doi.org/10.1109/ACCESS.2023.3308601.

[8] H. Amari, Z. A. E. Houda, L. Khoukhi, and L. H. Belguith, "Trust Management in Vehicular Ad-Hoc Networks: Extensive Survey," *IEEE Access*, vol. 11, pp. 47659–47680, 2023, https://doi.org/10.1109/ACCESS.2023.3268991.

[9] I. U. Din, K. A. Awan, and A. Almogren, "Secure and Privacy-Preserving Trust Management System for Trustworthy Communications in Intelligent Transportation Systems," *IEEE Access*, vol. 11, pp. 65407–65417, 2023, https://doi.org/10.1109/ACCESS.2023.3290911.

[10] A. Bibi *et al.*, "TR-Block: A Trustable Content Delivery Approach in VANET Through Blockchain," *IEEE Access*, vol. 12, pp. 60863–60875, 2024, https://doi.org/10.1109/ACCESS.2024.3386461.

[11] A. Malik, M. Z. Khan, S. M. Qaisar, M. Faisal, and G. Mehmood, "An Efficient Approach for the Detection and Prevention of Gray-Hole Attacks in VANETs," *IEEE Access*, vol. 11, pp. 46691–46706, 2023, https://doi.org/10.1109/ACCESS.2023.3274650.

[12] L. Xiong, Q. Li, L. Tang, F. Li, and X. Yang, "Blockchain-based conditional privacy-preserving authentication scheme using PUF for vehicular ad hoc networks," *Future Generation Computer Systems*, vol. 163, Feb. 2025, Art. no. 107530, https://doi.org/10.1016/j.future.2024.107530.

[13] H. Han, M. Zhang, Z. Xu, X. Dong, and Z. Wang, "Decentralized Trust Management and Incentive Mechanisms for Secure Information Sharing in VANET," *IEEE Access*, vol. 12, pp. 124414–124427, 2024, https://doi.org/10.1109/ACCESS.2024.3453368.

[14] M. A. Al Sibahee, V. O. Nyangaresi, Z. A. Abduljabbar, C. Luo, J. Zhang, and J. Ma, "Two-Factor Privacy-Preserving Protocol for Efficient Authentication in Internet of Vehicles Networks," *IEEE Internet of Things Journal*, vol. 11, no. 8, pp. 14253–14266, Apr. 2024, https://doi.org/10.1109/JIOT.2023.3340259.

[15] Z. Zeng, Q. Zhou, K. Wei, N. Yang, and C. Tang, "BCS-CPP: A Blockchain and Collaborative Service-Based Conditional Privacy-Preserving Scheme for Internet of Vehicles," *IEEE Transactions on Intelligent Vehicles*, vol. 9, no. 2, pp. 4130–4144, Feb. 2024, https://doi.org/10.1109/TIV.2023.3327364.

[16] Z. Ma *et al.*, "A Blockchain-Based Secure Distributed Authentication Scheme for Internet of Vehicles," *IEEE Access*, vol. 12, pp. 81471–81482, 2024, https://doi.org/10.1109/ACCESS.2024.3409361.

[17] C. Xu, P. Zhang, X. Xia, L. Kong, P. Zeng, and H. Yu, "Digital-Twin-Assisted Intelligent Secure Task Offloading and Caching in Blockchain-Based Vehicular Edge Computing Networks," *IEEE Internet of Things Journal*, vol. 12, no. 4, pp. 4128–4143, Feb. 2025, https://doi.org/10.1109/JIOT.2024.3482870.

[18] T. Nandy, R. Md Noor, R. Kolandaisamy, M. Y. I. Idris, and S. Bhattacharyya, "A review of security attacks and intrusion detection in the vehicular networks," *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 2, Feb. 2024, Art. no. 101945, https://doi.org/10.1016/j.jksuci.2024.101945.

[19] J. Akram, A. Anaissi, A. Akram, R. Singh Rathore, and R. H. Jhaveri, "Adversarial Label-Flipping Attack and Defense for Anomaly Detection in Spatial Crowdsourcing UAV Services," *IEEE Transactions on Consumer Electronics*, vol. 71, no. 1, pp. 2163–2174, Feb. 2025, https://doi.org/10.1109/TCE.2024.3448541.

[20] X. Lu *et al.*, "Blockchain-Enabled Secure Offloading for VEC: A Multi-Agent Reinforcement Learning Approach," *IEEE Transactions on Dependable and Secure Computing*, vol. 22, no. 3, pp. 2978–2995, May 2025, https://doi.org/10.1109/TDSC.2024.3523561.

[21] Z. Li, J. Gong, X. Xiong, and D. Wang, "Multi-Slot Secure Offloading and Resource Management in VEC Networks: A Deep Reinforcement Learning-Based Method," *IEEE Access*, vol. 13, pp. 4533–4546, 2025, https://doi.org/10.1109/ACCESS.2024.3524636.

[22] Y. Chen, J. Wu, S. Ye, W. Li, and Z. Xu, "Budget-Constrained Resource Allocation and Pricing in VEC: A MSMLMF Stackelberg Game With Contract Incentive Mechanism," *IEEE Internet of Things Journal*, vol. 12, no. 5, pp. 5050–5067, Mar. 2025, https://doi.org/10.1109/JIOT.2024.3486378.

[23] M. A. Al-Absi *et al.*, "Secure and Efficient High Throughput Medium Access Control for Vehicular Ad-Hoc Network," *Sensors*, vol. 21, no. 14, Jul. 2021, Art. no. 4935, https://doi.org/10.3390/s21144935.

[24] N. Gadde, R. Shivaswamy, R. B. H. Siddamal, G. Gowrishankar, G. T. Raju, and S. S. P. Vijay, "Hybrid resource optimization strategy in heterogeneous wireless networks," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 37, no. 2, pp. 829–838, Feb. 2025, https://doi.org/10.11591/ijeecs.v37.i2.pp829-838.

[25] E. C. P. Neto *et al.*, "CICIoV2024: Advancing realistic IDS approaches against DoS and spoofing attack in IoV CAN bus," *Internet of Things*, vol. 26, Jul. 2024, Art. no. 101209, https://doi.org/10.1016/j.iot.2024.101209.